



TITLE:

1)量子光学と量子情報処理の基礎  
(第42回 物性若手夏の学校(1997年  
度))

AUTHOR(S):

井元, 信之

---

CITATION:

井元, 信之. 1)量子光学と量子情報処理の基礎(第42回 物性若手夏の学校  
(1997年度)). 物性研究 1997, 69(3): 307-316

ISSUE DATE:

1997-12-20

URL:

<http://hdl.handle.net/2433/96241>

RIGHT:

# 量子光学と量子情報処理の基礎

井元 信之

NTT 基礎研究所

## 1 はじめに

近年、量子光学の分野における一つの傾向として、光の量子状態の制御や検出に関する研究が盛んになって来ている。たとえば光のスライジング (squeezing)、光子のサブポアソン分布 (sub-Poissonian distribution)、光子のアンチバンチング (anti-bunching)、二光子干渉 (two-photon interference)、量子非破壊測定 (quantum nondemolition measurement: QND 測定) などである。これらは、物質と光の相互作用の半古典論 — すなわち電子は量子力学的に扱うが光は古典的電磁波とみなす方法 — では説明できず、真の量子論 — すなわち光も第二量子化して扱う方法 — でなければ説明できない現象と言われている。このような分野が発達したのは技術の進歩により理論検証実験が可能になって来たことが背景にあるが、それだけではなく、通信・情報処理・計測などの応用の場面においても量子力学に基づく揺らぎが究極的性能限界を決めるような領域に入り始め、テクノロジーの側からからも量子力学的揺らぎの制御に興味を持たれるようになって来たからである。

量子力学に根ざす揺らぎをこのように好ましからざるものとして制御しようとする研究に対し、量子力学的揺らぎが持つ風変わりな性質 — 不確定性原理 (uncertainty principle)、重ね合せの原理 (superposition principle)、絡み合った状態 (entanglement) — を積極的に利用して、古典論の常識では考えられない情報処理を行おうという試みが最近とみに進展している。たとえば、直交しない複数の状態に信号を載せた場合、いかなる盗聴行為も信号の量子状態を変えてしまうことが重ね合せの原理から導かれるが、その変化を検知することにより盗聴痕跡のある乱数表とない乱数表を識別する量子暗号 (quantum cryptography) や、波動関数の並列処理性と状態表現の指数関数的多様性を巧みに利用して、膨大な計算量を少量の計算量に畳み込む量子コンピューティング (quantum computing) などである。量子暗号と量子コンピューティングは親戚関係にある分野と言えるが、後者は実現が技術的に難しいと認識されているのに対し、前者は有望視されている。

本講義では電磁場の量子化および関連基礎事項から始め、上述の分野を中心とする新しい研究の進展状況について解説する。そのために必要な基礎的概念について、本稿では物理的解釈に重きをおいて導入を試みる。

## 2 光の量子効果が現れる例

光の量子論の正統的導入法は、おそらく黒体輻射や自然放出から始め、物質と光の相互作用におけるエネルギーやりとりの離散性を論ずることであろう。それはスタンダードな教科書 [1] [2] に任せるとして、本稿では通信・計測・情報処理の立場に立った導入を試みる。

図 1 に示すように、レーザー光のように一見何の揺らぎもない光を光ディテクターで受け、得られる光検波電流の周波数成分をスペクトラムアナライザで観測すると、ディテクターの測定帯域内で — たとえば 1 GHz まで — 大きさが  $2e\bar{I}R$  ( $e$  は電子の電荷、 $\bar{I}$  は電流  $I$  の直流成分、 $R$  はスペクトラムアナライザの負荷抵抗) の白色雑音が観測される。これはショット雑音とよばれ、その由来は半古典論と光の量子論でそれぞれ次のように説明される。

半古典論：レーザー光自体は揺らぎのない古典的波であるが、ディテクターの電子が不確定性を持っているため、光が電子列へ変換されるときにランダムに変換される。これが光検波電流のショット雑音である。すなわち雑音源は光でなくディテクターにある。

量子論：レーザー光も電子も不確定性を持っているが、ディテクターで光が電子列へ変換される過程において電子の応答は測定帯域内では十分速いと仮定する。したがって電子列のランダム性は専ら光の不確定性を反映している。レーザー光は電子列に変換されるときに完全にランダムに変換されるような量子状態にある。すなわち雑音源はディテクターでなく光の量子状態にある。

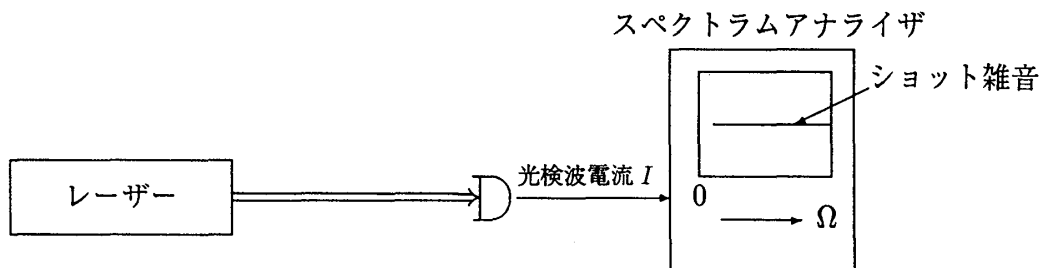


図 1. レーザー光の直接検波。スペクトラムアナライザ上には大きさ  $2e\bar{I}R$  の白色のショット雑音が観測される。

このようにショット雑音は半古典論と量子論のどちらでも説明できる。すなわち図 1 の実験系でショット雑音が観測されたとしても、その説明に光の量子論はことさら必要ではない。

次に図 2 のような実験系を考える。光パラメトリック変換器は非線形光学結晶からなり、周波数<sup>1</sup>  $\omega_p$  の光を受け  $\omega_s + \omega_i = \omega_p$  を満たす周波数  $\omega_s$  と  $\omega_i$  の光を発生する。添字  $p, s, i$  は慣例に従いそれぞれ ポンプ光 (pump)、信号光 (signal)、アイドラー光 (idler) を意味する。光の古典論では  $\omega_p$  の波が系の非線形応答により  $\omega_s$  と  $\omega_i$  の波に分解されるプロセスと理解され<sup>2</sup>、光の量子論ではエネルギー  $\hbar\omega_p$  ( $\hbar$  はプランク定数を  $2\pi$  で割ったもの) の光子 1 個が非

<sup>1</sup>慣例に従って本稿で周波数と呼ぶ  $\omega$  は正確には角周波数である。すなわち光の振動は  $e^{-2\pi i\omega t}$  でなく  $e^{-i\omega t}$ 。

<sup>2</sup>非線形光学現象の古典論は文献 [3] に詳しい。

線形光学結晶の中で  $\hbar\omega_s$  と  $\hbar\omega_i$  のエネルギーを持つ 2 つの光子に分解するプロセスと理解される。この信号光とアイドラー光をそれぞれディテクター  $D_s$  と  $D_i$  で受け、2 つの光検波電流  $I_s$  と  $I_i$  の差  $I$  をスペクトラムアナライザで観測する。

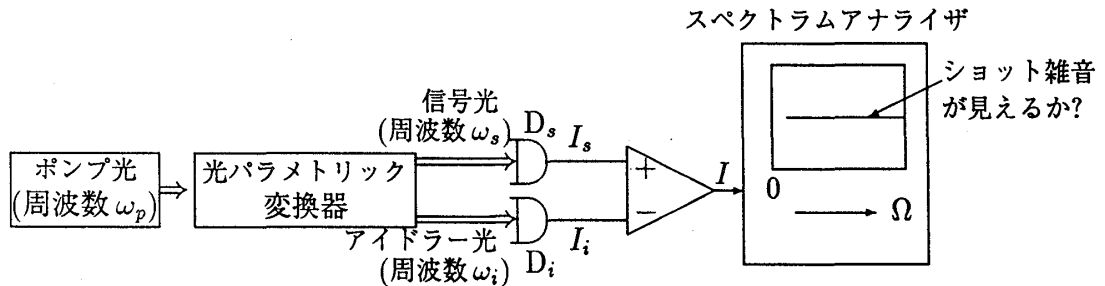


図2. パラメトリック変換器による信号光とアイドラー光の光検波電流  $I_s$  と  $I_i$  の差  $I$  の雑音測定系。スペクトラムアナライザ上にショット雑音が見えるか否かが問題。

この実験に対し半古典論と量子論では次のように異なる予想を与える。

半古典論：揺らぎのない  $\omega_p$  の波が分解した  $\omega_s$  と  $\omega_i$  の波にも揺らぎはない。ショット雑音はディテクター  $D_s$  と  $D_i$  で独立事象的に発生するので、 $I_s$  と  $I_i$  は相関のない雑音を持っている。したがって両者の差を取ると雑音エネルギーとしては和を取ることになり、スペクトラムアナライザには  $2e(\bar{I}_s + \bar{I}_i)R = 2e\bar{I}R$  のショット雑音が観測される。

量子論： $\omega_s$  と  $\omega_i$  の光子は必ずペアで出てくるので、 $I_s$  と  $I_i$  は同じ揺らぎを持っている。ディテクターでは余計な雑音は付加されないので、 $\bar{I}_s$  と  $\bar{I}_i$  が光子数に規格化されていれば  $2e(\bar{I}_s - \bar{I}_i)R = 0$  となり、スペクトラムアナライザには雑音は観測されない。

したがって図2の実験を行えば半古典論と量子論のどちらが正しいか判別できる。この実験は実際に行われ、その結果量子論の予想の方が正しいことが示された。すなわち図2の実験を説明するためには光の量子論が必要である。

図2の実験を計測や通信に応用するとすれば、次のような例が考えられる。レーザー光強度の微小変調成分を測定する必要があるとしよう。変調がショット雑音に埋もれてしまうほど浅ければ、通常は検出できない。しかし図2の系で信号光のみ変調がかかるようにすれば、 $I_s$  と  $I_i$  の差をとることにより、ショット雑音は大部分を落とすことができ、S/N比を大幅に改善できる。これは光強度の量子雑音を打ち消したことに相当する。この事情を詳しく見てみると、光強度の量子雑音を減らすためには、光強度と相補的な物理量である光位相を犠牲にする必要があることが分かる。不確定性原理は二つの相補的な物理量（たとえば位置と運動量）の不確定量の積について最小値を規定するが、それぞれの物理量を別個には規定しない。このように相補的な物理量の片方の雑音増加を代償にもう片方の雑音をショット雑音以下に抑えこむことを一般にスクイジングという。一つの物理量（この例では光強度）しか使わない場面では有効な方法である。

ここで次のような疑問が起こるであろう。すなわち、片方を犠牲にして一つの物理量の雑音を減らすのと、ある程度雑音を覚悟して二つの物理量を両方使うのとどちらが有利か、という問である。この問題は「平均光強度を一定としたとき、強度と位相の片方を犠牲にする方法と両方を使う方法ではどちらが多くの情報量を扱うことができるか?」と定式化される。「多くの情報量」を定量的に扱うのは相互情報量 (mutual information) と呼ばれる量で、これを最大化する変分問題を解くことになる。相互情報量については講義で説明することとして、ここでは上記の疑問の答が「片方を犠牲にする方が有利」であることだけを言っておこう。

### 3 光の量子化法

光の量子化は通常、仮想的体積  $V$  の中に充満する定常的電磁場のモードを定義することから始まる [1] が、量子光学のほとんどの実験では一次元軸に沿って伝搬する光ビーム — 空間ビームにせよ光ファイバー中の伝搬モードにせよ — を扱うので、ここではそれに合うやり方で記述する。

電磁場の Maxwell 方程式を操作すると、一次元伝搬電磁波の電場 3 成分と磁場 3 成分のうち独立な波動方程式に帰着するのは 2 つだけであることが分かる。光ビームの進行方向を  $z$  軸とすれば、一般には電場の  $z$  成分  $E_z$  と磁場の  $z$  成分  $H_z$  を独立成分に選ぶのが便利であり、このとき独立な波動は  $E_z = 0$  の TE 波と  $H_z = 0$  の TM 波に分けられる。次に簡単のため横方向 ( $xy$  方向) の依存性のない一様な平面波を考える<sup>3</sup>と、実は TE 波も TM 波も  $E_z = H_z = 0$  の TEM 波になってしまう。この場合は独立な 2 成分として  $E_x$  と  $E_y$  を選ぶのが便利であり、これらはそれぞれ  $x$  偏光と  $y$  偏光に対応する。ここでは  $y$  偏光のみ考え、以後添字を落とし  $E_y$  を  $E$  と書く。 $z$  方向に長さ  $L$  で周期的境界条件を課せば、光の波数  $k$  として取り得る値は  $2\pi/L$  の正整数倍であり、そのときの電場の空間依存性は  $e^{ikz}$  である。電場  $E$  はそれぞれの波数の電場を適当な複素振幅  $a_k$  で足しあわせ

$$E = \sum_k \sqrt{\frac{\omega}{2\varepsilon_0 LA}} a_k e^{ikz} + \text{c.c.} \quad (1)$$

と書ける。ただし  $\varepsilon_0$  は真空の誘電率、 $A$  は光ビームの断面積である。(1) 式では  $a_k$  は「作用の平方根」の次元を持つので、 $a_k$  を無名数にするため、量子論を少し先取りする形で、係数に  $\hbar$  を押し込めよう。さらに真空中では (多くの媒質中でも) 波数  $k$  と周波数  $\omega$  は比例関係にあるので、和を取る添字を  $\omega (= 2\pi c m/L)$  に変更すると、(1) 式は

$$E = \sum_\omega \sqrt{\frac{\hbar\omega}{2\varepsilon_0 LA}} a_\omega e^{ikz} + \text{c.c.} \quad (2)$$

と書かれる。 $a_\omega$  は周波数  $\omega$  の成分の (無次元の) 複素振幅である。体積  $LA$  中の  $\omega$  の成分のエネルギーは単位エネルギー  $\hbar\omega$  を  $a_\omega^* a_\omega (= |a_\omega|^2)$  倍したものである。ここまでは (恣意的に導入した  $\hbar$  を含んでいるが)、古典的電磁気学の世界である。

<sup>3</sup>実際の光ビームは横方向に一様でないが、それは必要になってから取り込めばよい。

電磁場の第二量子化は無次元複素振幅  $a_\omega$  を「光子の消滅演算子」 $\hat{a}_\omega$  と見なし、その複素共役  $a_\omega^*$  を「光子の生成演算子」 $\hat{a}_\omega^\dagger$  と見なすことによって行われる。すなわち周波数  $\omega$  の光子が体積  $LA$  中にきっかり  $n$  個存在する状態をケットベクトル記号  $|n\rangle_\omega$  で表したとき、 $\hat{a}_\omega|n\rangle_\omega = \sqrt{n}|n-1\rangle_\omega$  および  $\hat{a}_\omega^\dagger|n\rangle_\omega = \sqrt{n+1}|n+1\rangle_\omega$  が成り立つ。普通の数でなく演算子であることを示すためにハット<sup>^</sup>を用いている。光子の生成・消滅演算子には

$$[\hat{a}_\omega, \hat{a}_{\omega'}^\dagger] \equiv \hat{a}_\omega \hat{a}_{\omega'}^\dagger - \hat{a}_{\omega'}^\dagger \hat{a}_\omega = \delta_{\omega, \omega'} \quad (3)$$

の交換関係が成り立ち、光子数演算子  $\hat{n} = \hat{a}_\omega^\dagger \hat{a}_\omega$  は  $n + \frac{1}{2}$  ( $n$  は非負整数) の離散的固有値を持つ。係数  $\sqrt{\frac{\hbar\omega}{2\epsilon_0 LA}}$  は、いわば光子一つあたりの電場の大きさに相当する。電磁場のエネルギーを体積  $LA$  中で積分したものはハミルトニアン  $\hat{H}$  であり、これは

$$\hat{H} = \sum_\omega \hbar\omega \left( \hat{a}_\omega^\dagger \hat{a}_\omega + \frac{1}{2} \right) \quad (4)$$

となる。特に光子が一つもない状態 — 真空状態 — にも一モードあたり  $\hbar\omega/2$  のエネルギーが残り、これは零点エネルギーとか真空場の揺らぎ (zero point fluctuation あるいは vacuum fluctuation) などと呼ばれる。

## 4 光の量子状態と非古典的效果

光の量子状態が呈する非古典的效果には光子数のサブポアソン分布、ショット雑音以下の光検波電流雑音、光のアンチバンチングなどがある。通常のレーザー光はこれらの効果を示さない。それはレーザー光が「コヒーレント状態」と呼ばれる状態にあるからであり、コヒーレント状態が関与する現象の大部分は「古典的波である光をディテクターが受けたときにランダムに光電子を生起する」という半古典論で済むからである。以下ではコヒーレント状態の概略を述べ、それを基準に上記三つの効果が非古典的效果であることを見ていこう。

レーザー光は古典的には強度と位相が確定した光であるが、量子論では強度と位相が両方とも本当に確定した状態はない。古典的イメージとして両方が確定した状態を最もよく表す量子力学的光の状態は「コヒーレント状態」と呼ばれ、理想的レーザーが発する光の状態であり、それは消滅演算子の固有状態であることが知られている [2]。簡単のため周波数が決まっている単一のモードだけを考え、添字  $\omega$  を落とし、固有値  $\alpha$  に対するコヒーレント状態を  $|\alpha\rangle$  と書くと、 $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$  が成立する。 $\alpha$  は無次元の複素振幅であり、その絶対値の二乗は光子数の期待値を、その位相は光振動の位相の期待値を表す。状態  $|\alpha\rangle$  を光子数確定状態  $|n\rangle$  で展開すると、 $|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$  となる。したがってこの状態について光子数を測定した場合の光子数分布  $P_n$  は

$$P_n \equiv |\langle n|\alpha\rangle|^2 = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!} \quad (5)$$

となる。この分布をポアソン分布と言い、光子が完全にランダムに生起する場合の光子数分布である。この分布の特長は、分散が平均値に等しいというものである。ポアソン分布より鋭い

分布 — すなわち分散が平均値より小さい分布 — をサブポアソン分布という。光子計数の結果がサブポアソン分布になる光があったとすれば、それは半古典論では説明できず、光の量子論が必要である。したがって光子数のサブポアソン分布は光の量子状態が呈する効果と言わざるを得ない非古典的效果である。

コヒーレント状態の光では長さ  $L$  毎の波束に含まれる光子数がポアソン分布になっているので、図1のような光検波電流雑音の測定を行うと、 $L/c$  より遅い時間成分の雑音レベルはショット雑音レベルに一致する。 $L/c$  より速い時間成分で見ても、光電子の生起が全くランダムとすればやはりショット雑音に一致する。したがって一般にコヒーレント状態は量子化ビーム長  $L$  の取り方に依存せず、高い周波数まで<sup>4</sup>一定値のショット雑音を呈する。光検波電流がショット雑音より低くなることを光強度のスクイジングと呼ぶが、そのような光ビームがあったとすれば、それは半古典論では説明できない。したがって光強度のスクイジングは光の量子状態が呈する効果と言わざるを得ない非古典的效果である。

図1の実験系で光検波電流  $I(t)$  を測定して  $g^{(2)}(\tau) \equiv \langle I(t)I(t+\tau) \rangle / \langle I(t) \rangle \langle I(t+\tau) \rangle$  なる量を  $\tau$  の関数としてプロットしたとしよう。光ビームがコヒーレント状態だとすれば、光電子の生起は完全にランダムな事象と見なせるので、 $\tau$  によらず  $g^{(2)} = 1$  である。これは、ある時刻での光電子の生起と次の光電子の生起が全く独立事象であることを意味する。さらに光源に何らかの強度変動があるとすれば、 $g^{(2)}$  は変動の相関を表すので、 $\tau = 0$  の近辺で必ず  $g^{(2)}$  は1より持ち上がる。これは、ある時刻強い光が来ればその直後はやはり強い光が来る確率が高く、弱い光が来ればその直後はやはり弱い光であるという傾向を反映している。このように光電子がかたまって発生することをバンチングと言ひ、半古典論で十分説明できる現象である。これに対し  $\tau = 0$  の近辺で  $g^{(2)}$  が1より下がって観測された場合、それは一度光電子が生起すれば次の光電子はすぐには生起されないことを意味する。これを光のアンチバンチングと呼ぶ。アンチバンチングはディテクターが勝手に雑音を出しているという半古典論では説明できない。雑音の源は光の量子状態にあり、ひとたび光電子が生起すれば次の光電子はすぐには生起されないような量子状態であると解釈しなければならない。したがって光のアンチバンチングは光の量子状態が呈する効果と言わざるを得ない非古典的效果である。

## 5 量子非破壊測定

不確定性原理は通常波動関数そのものが持つものと考えられているが、それに上乗せされる形で測定する際にも課せられるものであることは意外と知られていない。すなわち二つの相補的物理量を同時に正確に測定する方法があれば、波動関数が持つ不確定性が生のまま見えるはずであるが、実際にはそのような測定方法はなく、どちらかを犠牲にするか、両方に量子雑音が入る形で両方を同時測定するかしかない。したがって測定値の不確定性は波動関数が持っている不確定性よりさらに大きくなる。測定に際して現れるこの不確定性原理は、もとを正せば、

<sup>4</sup>もちろん光の周波数そのものより高い周波数は意味がないが、通常の光ディテクターの帯域の範囲は問題ない。

被測定系に結合させられるプローブ系の量子状態の不確定性にその起源があるが、いずれにしても不確定性原理は量子状態の準備と測定<sup>5</sup>の二段階に現れる。前述のスライジングが量子状態の準備に際しての不確定性の操作であるとするれば、測定に際してのスライジング — すなわち一つの物理量の測定は諦めて他方を精度よく測定する測定法 — もあるはずである。比喩的に言えば、通常のスライジングが分布そのもののスライジングとすれば、測定精度の窓のスライジングもあるだろうというわけである。量子非破壊測定はそのような測定法の一つであるが、さらに条件が厳しくなっている。

量子非破壊測定とは「ある物理量の測定後の運動に攪乱を与えずにその物理量を測定する方法」である。英語の Quantum nondemolition measurement を略して QND 測定とも呼ばれる。条件が厳しくなっていると言ったのは、測定の瞬間だけでなく「測定後」の運動に攪乱を与えてはならないからである。この条件のために、原理的に量子非破壊測定できない物理量がある。例として自由粒子の位置の測定を考えてみよう。ある瞬間に位置を高精度で測定したとすれば、相補的物理量である運動量は不確定となる。運動量を粒子の質量で割ったものが速度であるので、これは測定後の速度が不確定となることを意味する。したがってその後の粒子の位置も不確定となる。自由粒子の運動量の測定の場合はこれとは事情が異なり、その後の運動量は測定値の値を保持する。このように量子非破壊測定が可能な物理量を QND 変数 (QND observable) と呼ぶ。位置が QND 変数でなく運動量が QND 変数であるという対称性の悪さは、自由粒子のハミルトニアンに位置は含まれず運動量のみが含まれるという事情による。光の場合、光子数 (光強度)、位相、複素振幅の実部 ( $\cos$  成分) と虚部 ( $\sin$  成分) が QND 変数である<sup>5</sup>。光子数 (光強度) の量子非破壊測定には光 Kerr 効果を用いる提案などがあるが、詳しくは講義で説明する。文献 [5] も参照されたい。

## 6 量子情報処理に入る前に

量子暗号や量子コンピューティングについては紙面の都合上本稿で詳しく説明することはできない。ここではその準備として、通常あまり指摘されないことであるが、持っている情報に依存して量子状態が一意でないことについて触れておきたい。

対象となる系の量子状態が一つの波動関数  $|\psi\rangle$  で表される場合、その量子状態は純粋状態と呼ばれ、適当に選んだ波動関数群  $|\psi_n\rangle$  の重ね合せで  $|\psi\rangle = \sum_n c_n |\psi_n\rangle$  で表される。波動関数群  $|\psi_n\rangle$  が直交基底をなし、それらに分解するような量子測定を  $|\psi\rangle$  に対し行ったらとすれば、特定の  $n$  の波動関数に見いだされる確率は  $|c|^2$  である。しかしこれは、もともと  $|\psi_n\rangle$  だったが知らなかっただけというのではない。重ね合せ状態は測定されるまでどの状態に落ち込むか本当に分からない状態と量子力学では解釈されている。一方  $|\psi_n\rangle$  のどれかであることがわかっているが、その確率  $p_n$  しか知らない場合は混合状態と呼ばれる。それは波動関数で表す

<sup>5</sup> 正確には位相を量子力学で扱うのは困難であるが、真空状態を含む割合が少ない光の場合はよい近似で位相を定義できる。



ことはできず、密度演算子  $\hat{\rho}$  で

$$\hat{\rho} = \sum_n p_n |\psi_n\rangle\langle\psi_n| \quad (6)$$

と表される。これに対し純粋状態  $|\psi\rangle$  に対する密度演算子は

$$\sum_n \sum_m c_n c_m^* |\psi_n\rangle\langle\psi_m| \quad (7)$$

で表される。これは量子力学の基本である。

本節では二つのことを指摘しておきたい。ひとつは、ある系の量子状態は客観的なものではなく、それに関する情報をどのくらい持っているか、人によって異なるということである。これは、ある系の量子状態は一つの密度演算子によって完全に定められ、その客観的状态を議論する通常の物理学の態度とは異なる。通常の物理では「自然」を観察する主体は一つで、我々は観察者として一体である。しかし情報処理では少なくとも情報の送り手と受け手の二つ以上の主体があり、しかもある場合は互いに信頼しあわない状況でゲームを行い、ある場合は互いにチームを組み、割って入ろうとする第三者に対抗しようとする。セキュリティ通信すなわち暗号は後者の代表例である。このような場合、量子状態を作って送る送り手にとっては当然純粋状態にある信号も、受け手が測定を行うまではそれは混合状態にある。量子暗号ではこのような量子信号のやりとりとは別に公開で行われる会話も伴うが、盗聴者がそれを聞く前と後では当然量子状態は異なる。別の例では、式(7)で与えられる純粋状態を測定したとして、ある測定値  $n$  を得れば、状態は新しく  $|\psi_n\rangle$  という純粋状態になったことを知るが、測定が行われた事実だけを知って測定値を知らなければ、新しい状態は式(6)で  $p_n = |c_n|^2$  とした混合状態になる。このように、一つの系の量子状態は主体毎に、また情報処理ステップ毎に異なる(初めから同じ情報を共有していたら通信や情報処理は意味がない)。量子暗号は、送り手が送った状態を盗聴者には意味不明の混合状態になるようにしたまま受け手は混合状態から純粋状態へと特定して行くプロセスと言える(特定して行くために必要な情報を公開の会話でやりとりする)。

もう一つは、上に  $\sum_n p_n |\psi_n\rangle\langle\psi_n|$  と表される状態は、 $|\psi_n\rangle$  のどれかであることが分かっているが、その確率  $p_n$  しか分からない場合だと述べたが、必ずしもそうではないということである。例として一つの光子の偏光状態が直線偏光であり  $x$  (横) か  $y$  (縦) か決まっているがどちらか全く知らない状態を考えよう。この状態は

$$\frac{1}{2}(|x\rangle\langle x| + |y\rangle\langle y|) \quad (8)$$

と表される。一方一つの光子の偏光状態が円偏光であり  $r$  (右回り) か  $l$  (左回り) か決まっているがどちらか全く知らない状態を考えよう。この状態は

$$\frac{1}{2}(|r\rangle\langle r| + |l\rangle\langle l|) \quad (9)$$

と表される。簡単な計算により、この二つの密度演算子は完全に一致することが分かる。すなわち、「どちらか決まっているが知らないだけ」という解釈は成り立たないことになる。量子

暗号はまさにこの事実を利用する。すなわち、送信者が直線偏光で信号を変調したか円偏光で変調したか知らなければ、与えられた密度演算子は全く同一で区別がつかない。したがって盗聴者は何の情報も得られない。もちろん受け手も何の情報も得られないが、受け手が直線偏光測定と円偏光測定をランダムに行い、送信者との事後の公開会話で基底の選択が一致した信号の測定値だけを残して後は捨てれば、受け手にはきちんと情報が伝達されているのである。

内容の詳細は講義で説明して行くが、ここでは基本となる概念を指摘しておいた。次に参考文献をいくつかリストアップしておくので、簡単なものには目を通しておくことを奨める。単行本はより深く理解を求めるときに有益であろう。

## 7 参考文献

本稿で挙げる参考文献は、オリジナリティーにクレジットを与えるためではなく、学習を始めるためのものであることを断っておく。したがって日本語版が得られるものを中心に挙げる。半古典論の範囲でレーザーや非線形光学などの量子エレクトロニクスを広く記述した書物としては [6] [3] が挙げられる。光の量子論に入るためにもこれらの書物の感覚を掴むことは有益である。[6] の終章には光の量子論も少し含まれる。光の量子論を含む体系的教科書としては [1] [2] が名著である。ただしこれらはスクイジング、量子非破壊測定などの近年の話題には触れていない。これらの話題に触れている書物としては [7] [8] [9] がある。トピック別小解説としては、拙著ではあるが [5](量子非破壊測定) [10](光パルス変調の量子力学的扱い) [11](量子測定に関する話題) を挙げておこう。

量子情報処理の方は教科書的なものはまだあまりないが、量子推定理論の立場でまとめたものとして [12] がある。量子暗号、量子コンピューティングとなると雑誌の解説記事くらいしかないが、量子暗号については [13] [14] がある。量子コンピューティングに関しては、英語だが現時点では [15] がベストで、日本語小解説としては [16] [17] がある。

## References

- [1] R. Loudon: *The Quantum Theory of Light*, 2nd Ed. Clarendon Press, Oxford, 1982 (小島忠宣・小島和子共訳「光の量子論」第2版, 内田老鶴圃, 1994).
- [2] M. Sargent III, M. O. Scully, and W. E. Lamb, Jr: *Laser Physics*, Addison-Wesley, Reading, 1974 (霜田光一・岩澤宏・神谷武志共訳「レーザー物理」, 丸善, 1978).
- [3] A. Yariv: *Quantum Electronics*, 3rd Ed., John Wiley & Son, New York, 1987; A. Yariv: *Introduction to Optical Electronics*, Holt, Reinhart and Winston, 1971 (多田邦雄・神谷武志共訳「光エレクトロニクスの基礎」, 丸善, 1974).

- [4] A. Heidmann, R. J. Horowicz, S. Reynaud, E. Giacobino, and C. Fabre: Phys. Rev. Lett. **59** (1987) 2555.
- [5] 井元信之: 「光の量子非破壊測定」 光学第 19 巻第 11 号 (1990)762.
- [6] 霜田光一、矢島達夫編著「量子エレクトロニクス (上巻)」裳華房 (1972).
- [7] 花村榮一「量子光学」 (岩波講座 現代の物理学) 岩波書店 (1992).
- [8] 山本喜久、渡部仁貴「量子光学の基礎」培風館 (1994).
- [9] 松岡正浩「量子光学」東京大学出版会 (1996).
- [10] 井元信之: 「波束を分断された光子の干渉」 光学第 22 巻第 9 号 (1993)544.
- [11] 井元信之: 「量子測定が多様性」 数理科学 第 34 巻 2 号 (1996)44.
- [12] 広田修「光通信理論」森北出版 (1985).
- [13] A. エカート / 井元信之訳: 「量子暗号への招待」 パリティ **7**, No.2(1992)26.
- [14] G. コリンズ / 井元信之訳: 「量子暗号は史上最強の暗号」 パリティ **8**, No.5(1993)31.
- [15] A. Ekert and R. Jozsa: Rev. Mod. Phys. **68**(1996)733.
- [16] B. Schwarzschild/ 細谷暁夫訳: 「量子コンピューターへの第一歩」 パリティ **11**, No.10(1996)50.
- [17] S. ハロシュ / 井元信之訳: 「量子コンピューティングー未果てぬ夢か?」 パリティ **12**, No.3(1997)45.